ISSN 2319 – 7595
Volume 8, No.2, March - April 2019
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/IJISCS/static/pdf/file/ijiscs26822019.pdf
https://doi.org/10.30534/ijiscs/2019/26822019

ATTRIBUTE BASED PRIVACY PROTECTION ON CLOUD COMPUTING WITH AUDITING SCHEME

Aswathy TD [1], Amrutha CP[2], Aparna Dinesh[3], Mariamma Thomas[4], Ms.Simy Mary Kurian[5]
Mangalam College of Engineering[12345], aswathydileep880@gmail.com[1], amruthapramod94@gmail.com[2]
aparnadinesh1210@gmail.com[3], mariathomas00000@gmail.com[4], simysunish@gmail.com[5]

ABSTRACT

Cloud computing provides a variety of services to our present technical areas. It is useful for both consumers and businesses to use applications without access their personal files. Security is an inevitable element of our cloud service. So we should check that our service provider can provide the security for our data. But a number of high-profile hacking cases will lead to different types of security problems on cloud. It mainly occurs in multi users cloud computing areas Cloud security is important in every field of users. Everyone wants to provide their information safe and secure. For this purpose here we can use attribute based encryption that is a type of public key encryption. Attribute based encryption allows data owners and users to encrypt and decrypt based on the personal attributes. But a crucial security aspect of attribute based encryption is collusion resistance. So we propose an audit scheme which provides a type of privacy protection on users and prevent from unauthorized access from hackers.

Key words: Attribute based encryption, CP-ABE, collusion attack, auditing scheme.

1. INTRODUCTION

Cloud computing is a method for delivering various services in which resources are retrieved from the Internet through web based applications. Rather than keeping files on a hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. Cloud computing is commonly used in today's IT world because of its high accessibility and availability.

Major threats to cloud security include data breach, data loss, account hacking, insecure application programming interfaces (APIs),poor choice of cloud storage provides and shared technology that can compromise cloud security. There are several types of encryption methods are used on cloud computing for providing security on users data and attributes. Out of these the most probably used method is attribute- based encryption. Attribute-based encryption is a public key cryptography in which the private key is used to decrypt data on certain user attributes such as position, place of residence, specialization field etc. The attribute can be any kind of information. But there is collusion attack may occur. So here we introduce a framework to detect collusion attacks in security protocols. As science and technology progressed, medicine became an inevitable part of research.

Medical thesis is an essential component in modern health care management. Health information at various levels could be generated from Medical thesis. Accurate and reliable information is needed for planning health care activities and health budgeting and this could be obtained only from these records. It improves the storage, retrieval, and sharing of the medical information more efficient. We focus on multiple data owner scenario.

From the user's perspective, the ability to utilize and access the resources on demand and the availability of the cloud are strong incentives for the usage of cloud. But there exist many security problems. The importance of data integrity has been highlighted by the following research works under different system and security models. The major issue related to security problem is collude attack.

So here introduce an auditing scheme for privacy protection on the data's stored on the cloud server. It checks the integrity of stored data by themselves. Through detailed security analysis, the owner's document is shown to be more secure.

The remainder of this paper is organized as follows. In section2, the related works are discussed. Section3, the proposed techniques are presented. In section4, Experiment result followed by Conclusion.

2. RELATED WORKS

There exists a problem over encrypted cloud data when personalized multi-keyword ranked search is used to check whether queried keywords where present or not.

With the help of semantic ontology Word Net they build a user interest model for individual user. Kaiping xue express a dynamic secure group sharing framework in public cloud computing. In his point of view instigate a novel and an extremely secure group sharing framework for public cloud, which can definitely make good use of the Cloud Servers' help which is an added advantage but the security and privacy of the people will be undoubtedly taken care of, that is no sensitive data will be exposed to attackers or assaulter or even the cloud provider.[1] The framework is a combination of both proxy signature, enhanced TGDH and proxy re-encryption both together into a single protocol. By applying the proxy signature technique, the group leader can definitely grant the privilege of managing the group to one or more chosen group members. [1] By the implementation of proxy re-encryption, the operations which are mostly computationally intensive can be delegated to Cloud Servers without providing any of the private information. Extensive security and performance analysis shows that our proposed scheme is highly efficient and satisfies the security requirements of the public cloud based on secure group sharing. [1]

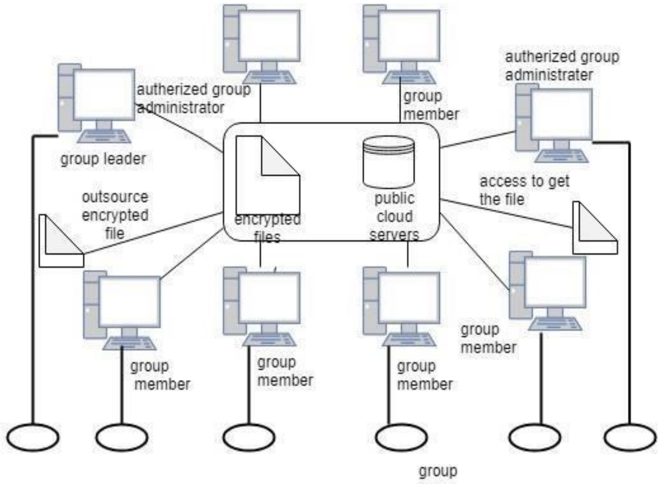

Figure 1: Data access control

Data access control using attribute based encryption in public cloud storage is the another related work which include Attribute Based Encryption (ABE), is a cryptographic system which gives data proprietor coordinate control over their data in public cloud storage. In the customary ABE conspire consists of single authority to keep up attribute set which can bring a solitary point change on both security and execution.

[2] Presently we utilize edge multi-authority Cipher content Policy Attribute-Based Encryption (CP-ABE) get to control plot, called by the name TMACS. TMACS is Threshold Multi-Authority Access Control System. In TMACS, different authority mutually deals with the entire attribute set but nobody has got the full authority to control a particular attribute.[2] By joining limit secret sharing (t,n) and multi-authority CP-ABE conspire, we have created a dynamic multi authority get to control framework in public cloud storage.[2]

The main advantage of Cipher text policy attribute based encryption algorithm is it provides fine grained and secure data access control for cloud storage (public) with cloud servers.

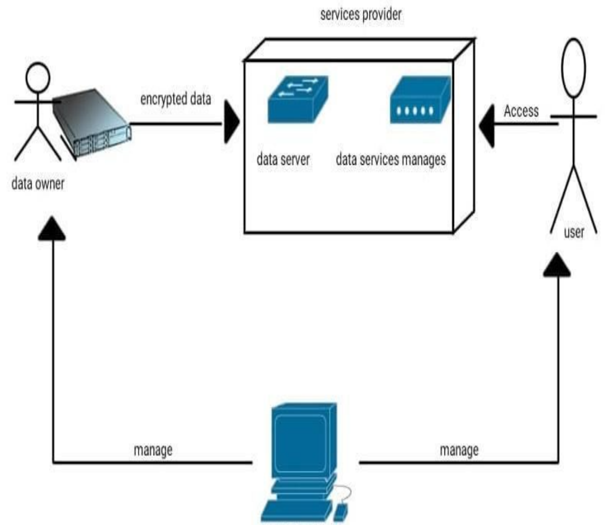

Figure 2: Data sharing system

But it has some flaws in its framework i.e. the single attribute authority must execute the time consuming user validation, verification and secret key distribution, and hence it results in a single point performance overhead.[3] When this technique is used in real time users have to wait in the waiting queue for a significant amount of time to obtain respective secret key, therefore it costs the efficiency of the system. This system cannot overcome the disadvantages of single point overhead efficiency. [4] Only one authority to maintain the whole attribute set in the earlier ABE scheme, but it can bring a single-point bottleneck on both security and performance.[5]

.

Some multiple authorities are subsequently proposed which multiple authorities are separately maintaining disjoint attribute subset. However, this problem remains unsolved that were shown by earlier ABE scheme.[6] A threshold multi-authority CP-ABE access control scheme for public cloud storage is known as TMACS, in which multiple authorities jointly manage a uniform attribute set. Security and performance analysis of the above system's results show that TMACS is not only verifiable secure when less than the authorities are compromised, but also robust when no less than the authorities are alive in the system.[3] Furthermore, the traditional multi-authority scheme with TMACS combined efficiently, we construct a hybrid one, which achieving security and system-level robustness.

From expressive efficient and revocable data access control , where there are multiple authorities co-exist and each authority is able to issue attributes independently.[5] Specifically, here a proposal for a revocable multi-authority CP-ABE scheme is made, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results demonstrate that the scheme is secure in the random oracle model. [7]

3. METHODOLOGY

For reducing the distribution complexity, the system is divided into multiple security attributes. Here the security is provided to the research papers of doctors belonging to five different countries. The security is provided in the attribute level. Hence each doctor has full control over their privacy. So key management complexity can be reduced. To implement and design a module based on attribute encryption, security is more provided. While using this attribute based encryption on cloud, it enhances the encrypted data. Here certificate authority can manage attribute authority and an auditing scheme is also provided for security purposes. The main problem is related to multiuser.

Cloud is collusion attack. This attack can be present to an extent by using this auditing scheme. This auditing scheme is a type of public key encryption .It is used to check the integrity of the users .So it maintains the documents and data without any modifications. The documents are visible to only authorized users and they cannot modify or download it.

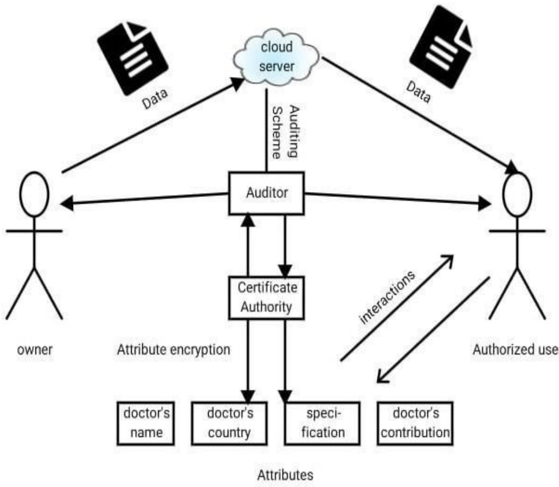

Figure 3: System architecture

Advantages

- Privacy is guaranteed by exploiting multi authority attribute based encryption.
- Data confidentiality.
- Write access control.
- Dynamic modification of access policies.
- On demand revocation.
- Scalable, secured and efficient.

4. EXPERIMENTAL ANALYSIS

From the analysis of each technology the security is improved from the beginning. Within the below shown graph, the X -axis imply that the gathering of records and the Y-axis represented that the percentage of accuracy of data. Thus the drawback is, as the security issues decrease the performance is also decrease. When compared to other technologies the auditing scheme provides more security. The feature of this auditing is to implement this with less time consumption. Collusion attack is a disadvantage that is seen in multiuser cloud service. And it can even prevent this at a limit through this new auditing scheme. By making use of the proxy signature approach, the group leader can successfully furnish the privilege of organization management to at least one or more selected group participants. If this server got any damage during the time of functioning that will affect the identity of the user.

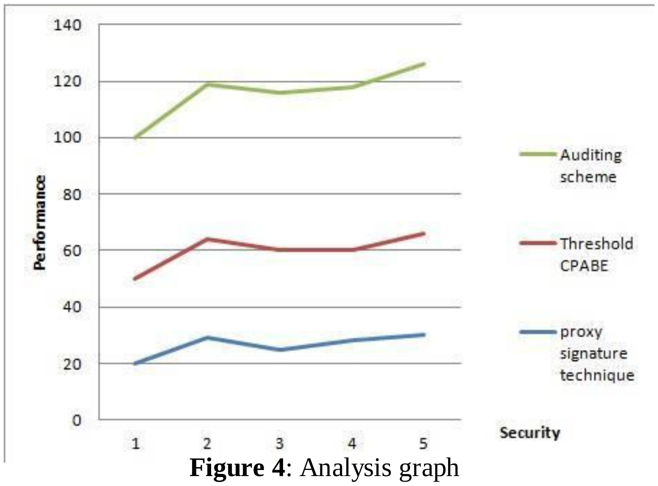

Figure 4: Analysis graph

The next technology access tree structure, the size of the cipher text in this technology is constant. If the size of the plain text is large, then the output of the corresponding size will not get. If use the Obfuscation technology, the data given by us is converted to another form and it will hide the existence of information. So the result is not an exact data. The loss of information is the major problem of this scheme. By the use of threshold multi authority CP-ABE scheme we can manage more than one authority with same attribute set. Multiple authorities share Master keys and it will generate Legal user's secret keys. When compared to other technologies this technology is more secure and robust.

Revocable multi authorities CP-ABE schemes are used to provide data access security ensure. Rather than that security can achieve both forward and backward.

5.CONCLUSION

An auditing scheme, which is based on attribute based encryption that provides extra security for the document stored in our cloud server. After some analysis, we classify the users according to their specialization in their studies and also in which country they are from. Here more security privacy is prevented for the documents. The security is based on the attribute level we constructed a new cipher text policy attribute based encryption (CP-ABE) with efficient encryption and decryption to avoid the collusion attack for some extent. The methodology and the analysis result shows that our new schemes are feasible and providing much security to the data stored in the cloud and it allows only authorized users to access the documents.

In future it will improve like currently we have added the data on cloud only but it can be stored in the big data scheme also. And the restriction to the file upload can be removed by supporting more file formats for videos audio image extras. The downloaded permission can be added to the existing view privilege.

REFERENCES

[1] .K. Yang and X. Jia, "Expressive, efficient and revocable data access control for multi-authority cloud storage," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 7, 2013. https://doi.org/10.1109/TPDS.2013.253

[2]. K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014. https://doi.org/10.1109/TCC.2014.2366152

[3]. J. Han, W. Susilo, Y. Mu, J. Zhou, and M. H. A. Au, "Improving privacy and security in decentralized cipher text policy attribute-based encryption," IEEE Transactions on Information Forensics and Security, vol. 10, no. 3, pp. 665–678, 2015 https://doi.org/10.1109/TIFS.2014.2382297

[4]. K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE Transactions on Parallel &Distributed Systems, vol. 26, no. 12, pp. 3461–3470, 2015. https://doi.org/10.1109/TPDS.2014.2380373

[5]. W. Li, K. Xue, Y. Xue, and J. Hong, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484– 1496, 2016. https://doi.org/10.1109/TPDS.2015.2448095

[6]. Kai Fan1*, Qiong Tian1, Junxiong Wang1, Hui Li1, Yintang Yang2, "Privacy Protection Based Access Control Scheme in Cloud-Based Services" IEEE/CIC ICCC, 2016.

[7]. CHEN D, SHAO J, FAN X, "MAH-ABE based Privacy Access Control in Cloud Computing", Chinese Journal of Electronics, vol. 42, no. 4, pp. 821-827, 2014.